NASA Technical Memorandum 104741

NASA-TM-104741 19920000818

Management of the Space Station Freedom Onboard Local Area Network

Frank W. Miller
Randy C. Mitchell

November 1991

NASA

NASA Technical Memorandum 104741

Management of the Space Station Freedom Onboard Local Area Network

Frank W. Miller
Lyndon B. Johnson Space Center
Houston, Texas

Randy C. Mitchell
Mitre Corporation
Houston, Texas

National Aeronautics and Space Administration
Lyndon B. Johnson Space Center
Houston, Texas

November 1991

CONTENTS

INTRODUCTION

This paper proposes an operational approach to managing the Data Management System (DMS) Local Area Network (LAN) on Space Station *Freedom*. An overview of the onboard LAN elements is presented first, followed by a proposal of the operational guidelines by which management of the onboard network may be effected. To implement the guidelines, a recommendation is then presented on a set of network management parameters which should be made available in the onboard Network Operating System (NOS) Computer Software Configuration Item (CSCI) and Fiber Distributed Data Interface (FDDI) firmware. Finally, a discussion of some implications for the implementation of the various network management elements is given.

ONBOARD LOCAL AREA NETWORK OVERVIEW

In the following overview of the onboard LAN subsystem, a description of the network elements including both hardware and software elements is given first. This is followed by a summary of the types of network traffic that are generated by these elements.

HARDWARE ELEMENTS

The onboard LAN consists of a set of processing nodes which communicate over an FDDI token ring network [3]. A node is an Orbital Replacement Unit (ORU) which is capable of transmitting to and/or receiving data from the network. The following is a list of the ORU node types considered in this paper:

1. Standard Data Processor (SDP)
2. Multipurpose Applications Console (MPAC)
3. Mass Storage Unit (MSU)
4. Gateway (GW)
5. Bridge (BR)
6. Intermediate Rate Gateway (IRGW)
7. Payload Processor

Although the approach to network management is similar for each of these node types, the specific requirements for the network management function in each type differ. This is due to different ORU node types containing different communications capabilities.

The communications function in each of the ORUs listed above is implemented using some configuration of Shop Replaceable Units (SRUs). In this paper, SRUs

can be thought of as printed circuit boards connected by a Multibus II backplane bus. The SRUs which are used in these ORUs are:

1. Embedded Data Processor (EDP)
2. Network Interface Adapter (NIA)
3. Intermediate Rate Gateway Adapter (IRGWA)

Figure 1 illustrates the specific configurations of these SRUs as they are utilized to implement the communications function in each ORU node type [4]. Each SDP, MPAC, MSU and payload processor contains a Network Interface Unit (NIU). An NIU consists of two SRUs, a Network Operating System (NOS) EDP and an NIA which connect to each other and to the other SRUs within each ORU by a Multibus II backplane. The U. S. side of the GWs consists of an NIA card and an NOS EDP card which connect to each other and the international's side of the GW by a Multibus II backplane. Each BR consists of two NIAs and an NOS EDP which are connected by a Multibus II backplane. Finally, the IRGW is assumed to consist of a special SRU which will be termed in this paper the IRGWA.

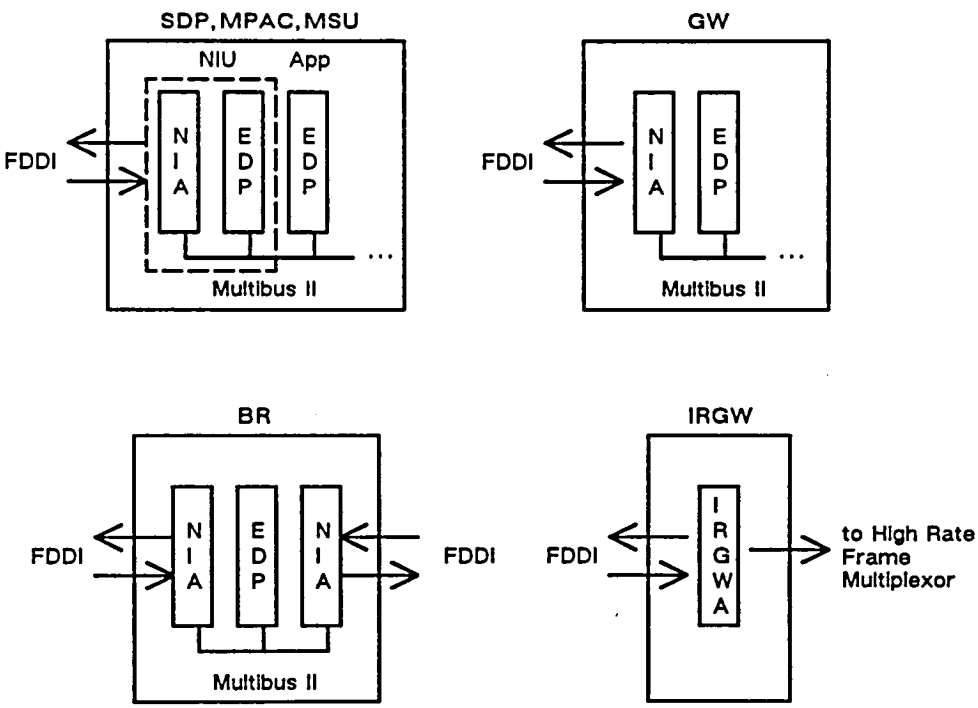

Figure 1
SRU Configuration for Each ORU Type

The following onboard communications subsystems are specifically excluded from consideration in this paper:

1. Communications and Tracking System (C&TS) space-ground communication elements
2. Audio and video communication elements
3. MIL-STD-1553B local busses and their attached elements
4. International Partner LAN elements
5. Ring Concentrators and passive elements such as the cable plant

Concepts from this paper may apply to the management of these subsystems, but they are not specifically considered here.

SOFTWARE ELEMENTS

The following software components are actively involved in the operation of the onboard LAN:

1. NIA Firmware [10]
2. IRGWA Firmware
3. Network Operating System (NOS) Software [11]
4. Standard Services (STSV) Software
5. Systems Management (SM) Software [13]
6. Data Storage and Retrieval (DSAR) Software

Firmware

Firmware resides in Read Only Memory (ROM) on an SRU card. When the SRU is powered on, the code in ROM is transferred to Random Access Memory (RAM) for execution. Specifications of the firmware for the NIA, BR, GW, and IRGW are in varying stages of development. The following descriptions make some assumptions about functions which must be included in those specifications.

NIA firmware resides in each NIA and is responsible for operating the protocols for NIA-to-NIA communication over the FDDI LAN media. These protocols together with the 802.2 Type I Link Layer Control (LLC) protocol [5] comprise layers 1 and 2 of the ISO Basic Reference Model [8]. The NIA firmware also operates the FDDI Station Management (SMT) functions and protocols, maintains the SMT Management Information Base (MIB) for layers 1 and 2 in each NIA, and makes the SMT MIB accessible to the Multibus II backplane.

The IRGWA firmware will be specialized for the high throughput requirement of that ORU. It will likely consist of only the FDDI and 802.2 Type I LLC protocols, and the code is likely to be highly optimized.

Software

Software is not initially present on an SRU when it is powered up. The SRU must execute an Initial Program Load (IPL) sequence in order to load required code into its RAM before beginning execution of its functions.

The NOS forms the basis of reliable communications on the LAN and resides in each NOS EDP. The NOS implements most of the protocols that provide the functionality of layers 3 through 7 of the ISO Basic Reference Model. The NOS also maintains an MIB for layers 3 through 7 in each NOS EDP that complies with the MAP/TOP 3.0 specification and makes its MIB and the NIA MIB accessible to Network SM.

STSV resides in each of the SDP EDPs, MPAC EDPs, and MSU EDPs on the LAN. STSV implements the protocol which is used to send telemetry over the C&T downlink [1] and initiates CMIS/CMIP [6] communications.

DSAR handles file accesses and transfers in the MSU. DSAR operates a file management protocol using NOS communication services. When ground or International Partner systems request file transfers to or from MSU disk storage, the file transfer is accomplished using the File Transfer Access and Management protocol [7].

Network SM resides in an MSU App EDP. Network SM maintains CMIS associations with the network management agents in all ORUs except the IRGW.

Note that traffic generated by the X Windows protocol is not considered in this paper. This protocol is at layer 7 but its interaction is with the layer 4 transport protocol rather than the normal layer 6 presentation protocol. When the specific use of this protocol is finalized, it can be considered in the same manner as the other layer 7 protocols mentioned in this paper.

TRAFFIC

Each node type has a different set of communications functions which must be managed. Figure 2 illustrates simplified diagrams of the functions for each type.

Observe that the SDPs, MPACs, and MSUs consist of two-way ISO/OSI layer 7 associations and a one-way layer 2 telemetry path onto the network. The GWs consist of two-way ISO/OSI layer 3 routing, a one-way layer 2 telemetry path from the International Partners LANs onto the U. S. LAN, and two-way ISO/OSI layer 7 associations which are used exclusively for network management. BRs are functionally equivalent to GWs. The difference is that BRs transfer data to and from the core and payload FDDI LANs within the U. S. portion of the Station. The IRGW consists of a one-way layer 2 telemetry path from the core LAN to the High Rate Frame Multiplexer (HRFM).

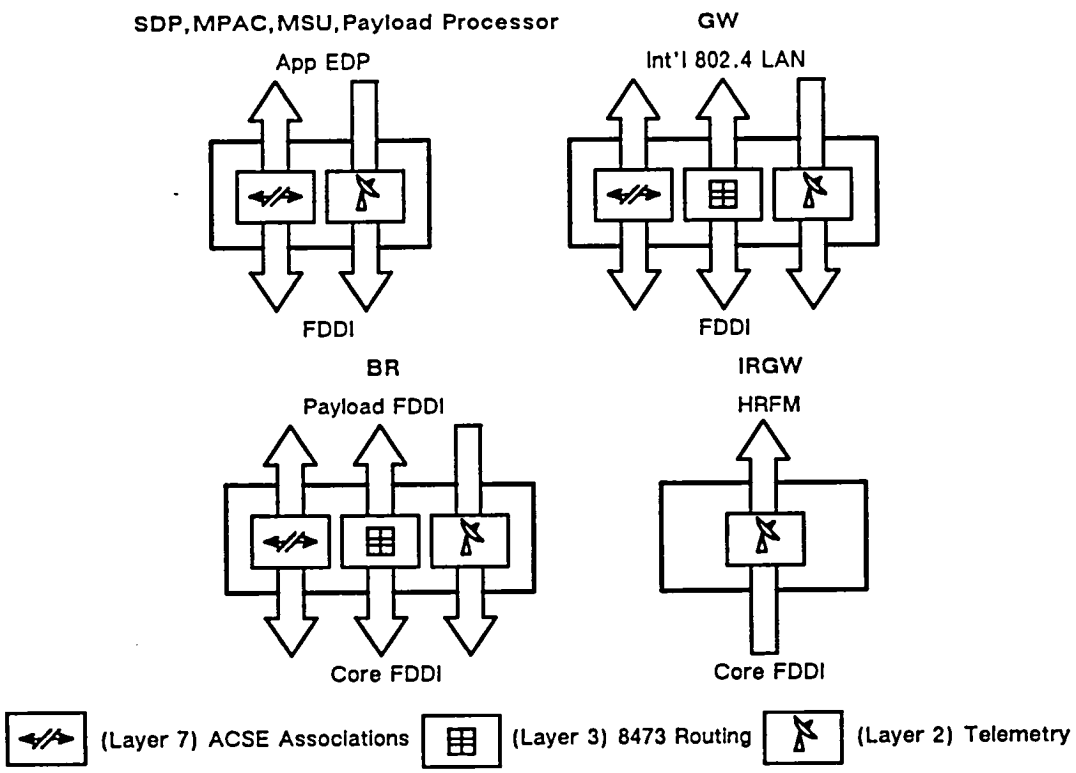

Figure 2
Communications Functions Required by ORU Node Types

Each of these communications functions generates a specific type of LAN traffic. Based on the functions illustrated in Figure 2, traffic on the LAN at a given instant can consist of any combination of any of the following four types:

1. Command/control (Layer 7)
2. ORU health and status (Layer 7)
3. File access and transfer (Layer 7)
4. Telemetry (Layer 2)

Note that no traffic is generated at layer 3. The layer 3 function included in the GW and BR ORUs is responsible only for routing data which is already on the LAN.

Data which traverses the LAN is generated by the SDPs, MPACs, MSUs, and payload processors as either layer 7 or layer 2 traffic. Although BRs and GWs are primarily responsible for routing of data at layer 3, it is important to note that they do generate *layer 7* network management data. The IRGW does not generate any network traffic, its only responsibility is to remove telemetry data from the LAN.

Telemetry will make up the largest portion of traffic which traverses the LAN. This traffic is generated by SDPs, MPACs, MSUs, and payload processors. The traffic takes the form of FDDI frames which enclose CCSDS packets that are destined for the ground. In the post-restructure DMS system, telemetry which is generated on the core LAN will be downlinked via the C&T Assembly/Contingency Baseband Signal Processor (ACBSP) which is attached to an SDP on the core LAN and all telemetry which is generated on the payload LAN is to be channeled to the C&T Ku band downlink through the IRGW which resides on the payload LAN.

Command and control data will utilize the reliable communications facilities provided by the ISO stack. This data must be guaranteed error free delivery. Command and control messages will be generated and received using this service by both onboard and ground systems. The post-restructure design calls for this data to traverse C&T by way of the ACBSP.

ORU health and status data will take several forms. There are low-level FDDI SMT packets which are periodically passed around the network in order to maintain operations. Those ORUs which contain an NIU will provide periodic health and status data to Network SM. There will likely be some form of "heartbeat" function which is implemented in the application processors (App EDPs) to maintain application operations. It is not clear at this time how frequent this data will be required or whether some portion of it will be telemetered to the ground.

Finally, file accesses and transfers will be very important for station operations. At the very least, executable images which are destined to be run on some processing node on the Station must be transferred to the onboard DMS system. In addition, the MSU file system capability will probably be used for a variety of other tasks. Traffic which is generated by file transfers will tend to be in bursts. However, when a file transfer is in progress, a significant portion of both the network and C&T bandwidth will be required to support it.

GUIDELINES FOR OPERATIONAL MANAGEMENT

The overriding concerns for the Station core LAN are that it be *available* and *reliable*. The LAN is available if processing nodes that are connected to it are able to communicate. Those communications are reliable if the data which is transmitted over the LAN are received without error and within specified latencies. It is the task of network management to assure that these two requirements are met.

A basic approach to implementing network management is proposed as follows. The LAN will be designed, developed, tested, and *tuned* on the ground prior to onorbit operations. While on orbit, a set of data regarding the status and performance of each node will be *monitored* during nominal operations in order to detect anomalous behavior. In addition, onboard nodes may generate asynchronous *events* indicating anomalous conditions. When an anomalous condition occurs, additional data may be *requested* and/or control *actions* may be executed in order to isolate the behavior. If an anomalous condition is detected and isolated, the failing node will be remove from the net and restarted in an attempt to correct the fault.

The following guidelines for management of the onboard LAN have been developed based on this basic operational approach:

1. No dynamic modifications of network performance parameters will be utilized during nominal operations. Performance of network nodes will be monitored only.
2. A minimal set of network management parameters will be monitored to detect and isolate anomalous behavior. Anomalous behavior must be isolated to the specific ORU(s) responsible for the anomaly.
3. Anomalous behavior will be manifest in two ways:
   A. Unplanned change in network configuration
   B. Unexpected performance degradation in at least one node
4. If an anomaly is detected and isolated to a specific onboard node, the recovery policy is to restart the communications elements of the node.

In the following sections, each of these guidelines is described in detail.

NOMINAL OPERATIONS

Nominal operations are defined as all onboard nodes being connected to the network and available to process their maximum throughputs. A specific

processing node is considered to be operating nominally if it is available to process all of its specific communication functions at their maximum throughputs.

The MAP/TOP 3.0 [9] and FDDI SMT [3] standards, which have been baseline for network management in the onboard LAN, provide a rich set of parameters which may be manipulated in order to provide desired response and performance from a network. Table 1 lists the number of parameters defined in these standards:

Table 1
Available Parameters for Network Management Standards

Standard	Attributes	Actions	Events
MAP/TOP 3.0	59	2	5
FDDI SMT	156	3	9

The intent of these standards is that the parameters be manipulated dynamically; that is, change the values of the parameters thereby modifying network performance while the network is in operation. For a man–rated spacecraft, this implies serious difficulties. Improper manipulation of parameters may result in unexpected behavior of not only the node where the parameters are modified but any other node with which it interacts.

It is therefore recommended that during nominal operations, *NO DYNAMIC MANIPULATION OF NETWORK PERFORMANCE PARAMETERS SHOULD OCCUR.* The network should be tested, tuned, and retested on the ground prior to onorbit operation. The only dynamic modifications allowed in the parameters specified in the following section concern changing routing tables. These parameters should be modified only to effect reconfiguration around a failure. If modifications are necessary in any of the other network parameters, a new executable image file should be transferred to the Station and the node should be reloaded.

NETWORK MANAGEMENT PARAMETERS

As noted, the network management standards define a large set of parameters which can be utilized to manage the network. If this approach to network operations is adopted, it is not necessary to make the entire set of network management parameters defined in the standards visible to external elements.

The following parameters comprise a recommendation for the set of data which will be necessary to effectively monitor the onboard LAN. For specific

descriptions of the parameters, refer to the MAP/TOP 3.0 or FDDI SMT standard. The parameters have been selected in an attempt to implement the guidelines proposed in the previous sections. They characterize primarily configuration and throughput data for each node connected to the LAN. Table 2 lists the parameters which have been selected from the MAP/TOP 3.0 standard, and Table 3 lists the parameters which have been selected from the FDDI SMT standard.

Table 2
MAP/TOP 3.0 External Interface Parameters

Parameter	Type	Use	Source	Dest
numberTPDUSent	Mon	F,P	NM	Gnd
numberTPDUReceived		F,P	NM	Gnd
numberOctetsSent		F,P	NM	Gnd
numberOctetsReceived		F,P	NM	Gnd
routingTable	Req	F	NM	Gnd,SM
advertizableCreditReduceZero		F,P	NM	Gnd
numberTPDURetransmitted		F,P	NM	Gnd
addRoutingTableEntry	Act	C	Gnd	NM,SM
deleteRoutingTableEntry		C	Gnd	NM,SM
ACSEThreshholdEvent	Evnt	F	NM	Gnd
presentationThreshholdEvent		F	NM	Gnd
sessionThreshholdEvent		F	NM	Gnd
transportThreshholdEvent		F	NM	Gnd
networkThreshholdEvent		F	NM	Gnd

Table 3
FDDI SMT External Interface Parameters

Parameter	Type	Use	Source	Dest
fddiSMTStationId	Mon	C	NM	Gnd,SM
fddiMACReceiveCt		F,P	NM	Gnd
fddiMACTransmitCt		F,P	NM	Gnd
fddiSMTCFState	Req	C	NM	Gnd,SM
fddiMACUpstreamNbr		C	NM	Gnd,SM
fddiSMTStationAction	Act	F,C	Gnd,SM	NM
fddiMACFrameErrorCondition	Evnt	F	NM	Gnd
fddiMACNotCopiedCondition		F	NM	Gnd
fddiMACNeighborChange		F,C	NM	Gnd,SM
fddiPortLerCondition		F	NM	Gnd
fddiConfigurationChgEvent		F	NM	Gnd,SM
fddiPortBERConditionEvent		F	NM	Gnd

There are four types of parameters, *monitored* (Mon), *requested* (Req), *actions* (Act), and *events* (Evnt). Monitored parameters are only generated by onboard nodes. The nodes will periodically sample the values of the parameters and report them to the destination. The period at which these parameters will be generated is

to be determined by the network system management application which will utilize them. The parameters selected are primarily concerned with throughputs in various layers of the communications stack. Requested parameters are also generated only by onboard LAN nodes. These parameters will be available to the specified destination on demand. Requested parameters may be used to assist in isolating network faults or assessing performance trends. Actions are commands which are sent to onboard nodes which affect their operations in some way. The most likely use of these parameters is to effect network configuration changes. Events represent asynchronous notification that some change has occurred in an onboard node. There are a wide variety of causes for the specified events to occur. Not all of the events are necessarily catastrophic.

The parameters listed in Tables 2 and 3 are used for three different facets or types of network management. Fault management (F) is primarily concerned with intranode failures such as incorrect checksums or protocol errors. Configuration management (C) refers to changes in the topology of the network. Performance (P) management is concerned with maintaining the maximum throughput capability for each communication function in each node.

Each parameter has associated with it an entity which is responsible for generating its values and an entity which will be responsible for receiving those values. These entities are listed as onboard node network management entities (NM), network System Management (SM), and ground systems (Gnd). NM refers to the MAP/TOP and FDDI SMT network management entities which run in each communications node. Network SM refers to that portion of Systems Management which is responsible for maintaining the overall network. This code resides in an onboard MSU ORU. Lastly, the Gnd will be required to provide systems that are capable of receiving and acting on the data generated by the onboard sources.

ANOMALOUS BEHAVIOR

Anomalous behavior will be observed as an unplanned change in the configuration of the network or an unexplained degradation in the performance of a node. The first type of anomaly is generally more serious than the latter.

Unplanned Change in Configuration

An unplanned change in network configuration indicates that one of the following events has occurred:

1. The FDDI ring has reconfigured itself
2. An active node has disconnected from the network
3. A previously inactive node has connected to the network

Reconfiguration of the FDDI LAN happens when the LAN utilizes the dual rings to wrap around a network fault. A wrap of the FDDI LAN as defined in the standard need not interrupt nominal operations. The intent of the FDDI standard is to allow network operations to continue in the presence faults. The crew and ground controllers may initiate actions which allow the ring to recover to its original configuration, but that action need not begin immediately. A reconfiguration of the FDDI ring simply means that the level of fault tolerance in the network has been reduced.

If a node disconnects from the LAN, the cause must be isolated. This may be difficult, however, because there is no path to communicate with the node since it is no longer connected to the network. Currently, the only course available to recover the node would be to cycle power on the ORU. When the node powers up, it will attempt to reconnect itself to the network as part of its initialization.

If a node unexpectedly connects to the network, the task of isolating the cause of the fault should be more straightforward. Monitored NM data may be analyzed and additional NM data may be requested from the node in order to narrow down the potential causes for connection. It should be possible to command the node to disconnect.

Unexplained Degradation in Performance

Degradation of throughput performance may or may not indicate a catastrophic failure in the network. A variety of traffic types traverse the LAN at a given instant, and the characteristics of the sources of each type of data as described in the previous sections may result in throughput problems.

The crew and ground controllers who monitor the onboard LAN must be aware of how application traffic affects throughput in each node. This requires training in network operations and knowledge of the mechanisms which implement onboard applications. When throughput degradation does indicate some catastrophic

fault, those responsible for monitoring the network can use throughput degradation data to assist in isolating the source and cause of the failure.

A separate activity is currently under way to address the most likely cause for throughput degradation. Local flow control in the onboard systems will be essential to avoid the problem. Results of that work are forthcoming.

RECOVERY

Currently, the requirements for the onboard LAN are to isolate network faults to the specific ORU where the fault occurred. Once the fault has been isolated, the proposed course of action to correct the fault is to restart the node.

A restart of a network node has implications for the entire system. While restarting connectionless services is relatively transparent to the operation of the overall system, this is not the case for connection-oriented or layer 7 services. Once the software has be restarted, those connections, which had previously passed through the node, must be reestablished. It is the task of the Network SM software element to initiate this task.

In the current design, a restart of the communications elements implies that power for the entire ORU must be cycled, and an IPL of the software for the ORU must then be completed. This approach to fault recovery will require significant time and DMS resources. There may be cases when the fault does not require actions be taken which affect the application functions running in an ORU. The relatively short duration required for a simple restart of the node's NIU software and firmware would certainly be preferable to the duration required to reload and restart the entire ORU.

As such, it is proposed that *the capability to perform an independent restart of communications software be implemented in those ORUs which contain SRUs that perform functions other than network communications.* This set of ORU types consists of any ORUs that use the NIU. The ORU types that qualify under this definition include all SDPs, MPACs, MSUs, and any payload processors which use the NIU elements.

Such a capability will affect the design of a number of DMS elements including the following:

1. NIU hardware: A mechanism for interrupting the software which runs in both the NIA and NOS EDP SRUs must be implemented.

2. NIU software: Restarting the NIA firmware and NOS software in an ORU should completely discard any communications which have been initiated at the time a restart signal is received.

3. SM: Must reestablish any ISO associations which were destroyed as a result of the restart. SM must also be responsible for containing the effects of the restart by managing the reactions of any elements in other nodes which were interacting with the restarted node.

In the other node ORU types, a restart can be effectively implemented by cycling the power for the ORU. This set of ORUs includes the GWs, BRs, and the IRGW. The GWs and BRs perform communications functions only. No gain would be realized by implementing an independent restart capability. The IRGW executes exclusively from firmware which can be reloaded quickly from Electrically Programmable Read-Only Memories (EPROMs).

CONCLUSIONS

In this paper, a basic approach to the task of operational network management of the Space Station onboard network has been presented. This approach is based on a philosophy which views the network elements as "black boxes" which, once built, tested, and tuned, should require little nominal maintenance from the crew or ground controllers.

To implement this approach, a number of significant proposals have been made:

1. No dynamic modifications to the network should be effected during nominal operations.
2. The minimal set of network management parameters selected from the MAP/TOP 3.0 and FDDI SMT standards and presented in this paper should be used to monitor and control the network.
3. A specific first course of action prescribed for correcting operational failures in network nodes is to restart the node.

This paper was generated as a result of a number of meetings between the authors and Work Package 2 (WP2) contractors, including members of the McDonnell

Douglas Space Station Division and members of the IBM Federal Sector Division. The authors would like to acknowledge Angelo Prevete, Hal Devore, Augie Mena, Jim Dashiell, and Dan Minear for their assistance.

REFERENCES

[1] Consultative Committee for Space Data Systems, Advanced Orbiting Systems, Networks and Data Links: Architectural Specification, CCSDS 701.0-R-3, 1989.

[2] Architectural Control Document, Data Management System, JSC 30261, 1991

[3] Fiber Distributed Data Interface, ANSI X3T9.5, 1990.

[4] Summary Presentation, Technical Interchange Meeting, IBM Federal Sector Division, May 1991.

[5] Information Processing Systems - Local Area Networks - Part 2: Logical Link Control, ISO DIS 8802-2, 1987.

[6] Information Processing Systems - Open Systems Interconnection - Common Management Information Service/Protocol, ISO 9595/9596, 1990.

[7] Information Processing Systems - Open Systems Interconnection - File Transfer, Access, and Management, ISO 8751, 1988.

[8] Information Processing Systems - Open Systems Interconnection - Basic Reference Model, ISO 7498, 1984.

[9] MAP 3.0 Implementation Release, MAP/TOP 3.0, 1987.

[10] Firmware Requirements Specification - Network Interface Adapter

[11] Software Preliminary Design Document - Network Operating System

[12] System Requirement Specification - Network Operating System

[13] System Requirement Specification - Systems Management

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	November 1991	Technical Memorandum

4. TITLE AND SUBTITLE
Management of the Space Station Freedom Onboard Local Area Network

5. FUNDING NUMBERS

6. AUTHOR(S)
Frank W. Miller and Randy C. Mitchell

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Flight Data Systems Division
National Aeronautics and Space Administration
Johnson Space Center
Houston, Texas 77058

8. PERFORMING ORGANIZATION REPORT NUMBER
S-649

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, D. C. 20546-001

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
NASA-TM-104741

11. SUPPLEMENTARY NOTES
Frank W. Miller, Johnson Space Center, Houston, Texas
Randy C. Mitchell, Mitre Corporation, Houston, Texas

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Unclassified/Unlimited Publicly available
Subject Category 17

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This paper proposes an operational approach to managing the Data Management System Local Area Network on Space Station Freedom. An overview of the onboard Local Area Network elements is presented first, followed by a proposal of the operational guidelines by which management of the onboard network may be effected. To implement the guidelines, a recommendation is then presented on a set of network management parameters which should be made available in the onboard Network Operating System Computer Software Configuration Item and Fiber Distributed Data Interface firmware. Finally, some implications for the implementation of the various network management elements are discussed.

14. SUBJECT TERMS
orbital replacement unit, local area network, network management parameters, file management protocol, fiber distributed data interface, telemetry path/data, anomalous behavior

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL